

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
INFORMATION ASSOCIATED WITH TWO
EMAIL ACCOUNTS THAT ARE STORED AT
PREMISES CONTROLLED BY MICROSOFT

Case No. MJ20-206

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-2, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-2, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1958	Murder for Hire

The application is based on these facts:

☒ See Affidavit of Allana Kleinosky, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

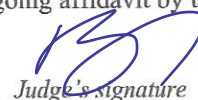
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Allana Kleinosky, Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 4/23/20


Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge
Printed name and title

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

INTRODUCTION AND AGENT BACKGROUND

2. Prior to my role as a Special Agent for the FBI, I was an Air Marshal with the Federal Air Marshal Service for three years and a Customs and Border Protection Officer with Customs and Border Protection for three and a half years. During my time as a Customs and Border Protection Officer and Federal Air Marshal, I participated in several arrests, seizures, and other law enforcement actions. I have conducted hundreds of interviews, have taken law enforcement action, and made law enforcement determinations based on the facts I gathered from these interviews.

3. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Microsoft Corporation (“Microsoft”), located at 1 Microsoft Way in Redmond, Washington, and Grays Harbor College, located at 1620 Edward P. Smith Drive in Aberdeen, Washington (collectively, “**THE PROVIDERS**”). The information to be searched is described in the following paragraphs and in Attachments A-1 and A-2.

4. This affidavit is made in support of an application for a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **THE PROVIDERS** to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachments B-1 and B-2, pertaining to the following accounts:

a. lfigueroa@my.ghc.edu (“**SUBJECT ACCOUNT 1**”);

b. prinhces_latina07@hotmail.com (“**SUBJECT ACCOUNT 2**”);

and

c. lluvia_selene07@hotmail.com (“**SUBJECT ACCOUNT 3**”);

(hereinafter, collectively the “**SUBJECT ACCOUNTS**”). Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2. This warrant is requested in connection with an ongoing investigation in this district by the FBI.

5. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1958 (Murder for Hire) have been committed by LLUVIA FIGUEROA. Section 1958 prohibits “us[ing] or caus[ing] another . . . to use . . . any facility of interstate or foreign commerce, with intent that a murder be committed in violation of the

laws of any State or the United States as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value” or conspiring to do the same. There is also probable cause to search the information described in Attachments A-1 and A-2, for evidence, instrumentalities, or contraband of these crimes, as described in Attachments B-1 and B-2.

7. This warrant application is to be presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

BACKGROUND ON CRYPTOCURRENCY

8. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.¹ Cryptocurrency is not illegal in the United States.

9. Bitcoin² is a type of cryptocurrency. Payments or transfers of value made with bitcoins are recorded in the Bitcoin blockchain and thus are not maintained by any

¹ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

² Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and

1 single administrator or entity. As mentioned above, individuals can acquire bitcoins
2 through exchanges (i.e., online companies which allow individuals to purchase or sell
3 cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), Bitcoin
4 ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by
5 “mining.” An individual can “mine” bitcoins by using his/her computing power to solve
6 a complicated algorithm and verify and record payments on the blockchain. Individuals
7 are rewarded for this task by receiving newly created units of a cryptocurrency.
8 Individuals can send and receive cryptocurrencies online using many types of electronic
9 devices, including laptop computers and smart phones.

10 10. Even though the public addresses of those engaging in cryptocurrency
11 transactions are recorded on a blockchain, the identities of the individuals or entities
12 behind the public addresses are not recorded on these public ledgers. If, however, an
13 individual or entity is linked to a public address, it may be possible to determine what
14 transactions were conducted by that individual or entity. Bitcoin transactions are
15 therefore sometimes described as “pseudonymous,” meaning that they are partially
16 anonymous. And while it is not completely anonymous, Bitcoin allows users to transfer
17 funds more anonymously than would be possible through traditional banking and credit
18 systems.

19 11. Cryptocurrency is stored in a virtual account called a wallet. Wallets are
20 software programs that interface with blockchains and generate and/or store public and
21 private keys used to send and receive cryptocurrency. A public key (or public address) is
22 akin to a bank account number, and a private key (or private address) is akin to a Personal
23 Identification Number (“PIN”) number or password that allows a user the ability to
24 access and transfer value associated with the public address or key. To conduct
25 transactions on a blockchain, an individual must use the public key and the private key.

26
27
28 community, and “bitcoin” (with a lowercase letter b) or “BTC” to label units of the
cryptocurrency. That practice is adopted here.

1 A public address is represented as a case-sensitive string of letters and numbers. Each
2 public address is controlled and/or accessed through the use of a unique corresponding
3 private key—the cryptographic equivalent of a password or PIN—needed to access the
4 address. Only the holder of an address’s private key can authorize any transfers of
5 cryptocurrency from that address to another cryptocurrency address.

6 12. Although cryptocurrencies such as Bitcoin have legitimate uses,
7 cryptocurrency is also used by individuals and organizations for criminal purposes such
8 as money laundering, and is an oft-used means of payment for illegal goods and services
9 on hidden services websites operating on the Tor network. By maintaining multiple
10 wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law
11 enforcement’s efforts to track purchases within the dark web marketplaces.

12 13. Exchangers and users of cryptocurrencies store and transact their
13 cryptocurrency in a number of ways, as wallet software can be housed in a variety of
14 forms, including: on a tangible, external device (“hardware wallet”); downloaded on a
15 Personal Computer (“PC”) or laptop (“desktop wallet”); with an Internet-based cloud
16 storage provider (“online wallet”); as a mobile application on a smartphone or tablet
17 (“mobile wallet”); as printed public and private keys (“paper wallet”); and as an online
18 account associated with a cryptocurrency exchange. Because these desktop, mobile, and
19 online wallets are electronic in nature, they are located on mobile devices (e.g., smart
20 phones or tablets) or at websites that users can access via a computer, smart phone, or any
21 device that can search the Internet. Moreover, hardware wallets are located on some type
22 of external or removable media device, such as a Universal Serial Bus (“USB”) thumb
23 drive or other commercially available device designed to store cryptocurrency (e.g.
24 Trezor, Keepkey, or Nano Ledger). In addition, paper wallets may contain an address
25 and a QR code³ with the public and private key embedded in the code. Paper wallet keys
26 are not stored digitally. Wallets can also be backed up into, for example, paper printouts,
27

28 ³ A QR code is a matrix barcode that is a machine-readable optical label.

1 USB drives, or CDs, and accessed through a “recovery seed” (random words strung
2 together in a phrase) or a complex password. Additional security safeguards for
3 cryptocurrency wallets can include two-factor authorization (such as a password and a
4 phrase).

5 **BACKGROUND CONCERNING THE DARK NET**

6 14. The “dark net” or “dark web” is a portion of the “Deep Web” of the
7 Internet, where individuals must use anonymizing software or applications to access
8 content and websites. Within the dark web, criminal marketplaces operate, allowing
9 individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous
10 materials, with greater anonymity than is possible on the traditional Internet (sometimes
11 called the “clear web” or simply the “web”). These online market websites use a variety
12 of technologies, including the Tor network (defined below) and other encryption
13 technologies, to ensure that communications and transactions are shielded from
14 interception and monitoring. Famous dark web marketplaces, also called Hidden
15 Services, such as Silk Road, AlphaBay,⁴ and Dream Market⁵ operated similarly to clear
16 web commercial websites such as Amazon and eBay, but offered illicit goods and
17 services. There are a number of marketplaces that have appeared on the dark web that
18 have offered contraband for sale, including narcotics. Users typically purchase narcotics
19 through these marketplaces using digital currency such as bitcoin.

20 15. “Vendors” are the dark web’s sellers of goods and services, often of an
21 illicit nature, and they do so through the creation and operation of “vendor accounts” on
22 dark web marketplaces. Customers, meanwhile, operate “customer accounts.” Vendor
23 and customer accounts are not identified by numbers, but rather monikers or “handles,”
24

25 _____
26 ⁴ AlphaBay was a website on the dark web that offered drugs and other contraband for sale.
Furthermore, I know that AlphaBay was seized by U.S. law enforcement in July 2017.

27 ⁵ Dream Market was a website on the dark web that offered drugs and other contraband for sale.
28 In late March 2019, Dream Market announced it was closing on April 30, 2019 and transferring
its services to a partner company.

1 much like the username one would use on a clear web site. If a moniker on a particular
2 marketplace has not already been registered by another user, vendors and customers can
3 use the same moniker across multiple marketplaces. Based on customer reviews, vendors
4 can become well known as “trusted” vendors.

5 16. The Onion Router or “Tor” network is a special network of computers on
6 the Internet, distributed around the world, that is designed to conceal the true Internet
7 Protocol (“IP”) addresses of the computers accessing the network, and thereby the
8 locations and identities of the network’s users. Tor likewise enables websites to operate
9 on the network in a way that conceals the true IP addresses of the computer servers
10 hosting the websites, which are referred to as “hidden services” on the Tor network.
11 Such “hidden services” operating on Tor have complex web addresses, which are many
12 times generated by a computer algorithm, ending in “.onion” and can only be accessed
13 through specific web browser software designed to access the Tor network. Most
14 “hidden services” are considered dark web services with no legitimate or identified
15 service provider to which legal process may be served.

16 **STATEMENT OF PROBABLE CAUSE**

17 **A. Summary of Investigation**

18 17. On February 12, 2020, the FBI received an anonymous tip from an
19 individual (“SOI-1”) purporting to operate a website on the dark web that offers hitmen
20 for hire. SOI-1 claimed to have received a request to murder a woman who resides in
21 Bellevue, Washington (“VICTIM”). SOI-1 stated that, although SOI-1’s website offers
22 to murder individuals in exchange for Bitcoin, the website is a scam, designed to steal
23 money from customers.

24 18. As described herein, the FBI has determined that, around the time of the
25 murder for hire, VICTIM’s husband, J.M., had been having an extramarital affair with
26 LLUVIA FIGUEROA, a college student whom he met at a self-help course. When the
27 FBI interviewed FIGUEROA, she admitted that she paid an unknown person, located on
28 the dark web, to kill VICTIM in exchange for \$5,000 in bitcoin.

19. As described in further detail below, FIGUEROA used **SUBJECT ACCOUNTS 2 and 3** to register a Facebook account. FIGUEROA used that Facebook account and **SUBJECT ACCOUNT 1** to communicate with J.M. during the course of the affair. FIGUEROA also used **SUBJECT ACCOUNT 2** to communicate with financial institutions and the cashier at Grays Harbor College. These emails may reveal the source of the funds used, including those transferred from J.M. and scholarship funds, to pay SOI-1 to murder VICTIM.

B. Anonymous Tip

20. On February 12, 2020, a complainant, SOI-1, submitted an online tip to the FBI National Threat Operations Center. The tip was anonymous, sent from a ProtonMail account, using an IP address associated with a Virtual Private Network (“VPN”)⁶ in Phoenix, Arizona. Based on my training and experience, and information gained during the course of this investigation, I know that individuals often use VPNs and encrypted email providers like ProtonMail in order to conceal their identities or physical locations online.

21. In this tip, SOI-1 claimed to have information regarding a murder for hire. SOI-1 claimed to be the administrator of a “dark web site that offers hitmen for hire,” and explained that he/she was contracted to kill VICTIM for approximately \$5,000, paid in bitcoin.⁷ SOI-1 claimed the website was set up to scam people out of money, and that no actual murders were committed by SOI-1 or anyone working on SOI-1’s behalf.

⁶ A VPN connection is a means of connecting to a private network over a public network such as the Internet. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. VPNs are also frequently used by people who wish to circumvent geographic IP limitations and censorship, and to connect to proxy servers for the purpose of obfuscating the source of an internet connection or transmission.

⁷ SOI-1 also informed the FBI about a second murder that had been solicited on SOI-1’s website unrelated to the VICTIM identified in this Affidavit. The FBI is also investigating that potential hit.

22. SOI-1 explained that he/she was concerned about receiving the request to murder VICTIM, thinking that if someone was willing to pay SOI-1, that person may find other means to kill VICTIM. SOI-1 wanted to work with the FBI and police to track down the individual who had solicited the murder. SOI-1 stated "I feel that all targets that have been paid for are in danger. Customers that pay to kill someone show that they are serious about killing that person[.] I need to be in contact with you and to provide you with the target information, payments evidence, and other information to trace the customers. Customers don't give their name or details and hide their IP, but still can be tracked." SOI-1 provided information related to VICTIM and another contract, and said he/she would be willing to provide more details on additional targets.

23. SOI-1 said that when he/she had received a request to murder VICTIM, the solicitor of this murder (hereinafter referred to as the "solicitor") provided SOI-1 with VICTIM's address in Bellevue, Washington, the name of her employer, the city where she was employed, the age of her son, her routine regarding child care, and the time she returns home. The solicitor told SOI-1:

Just kill her ASAP. I don't care how just make sure she's dead. I'd prefer if you shoot her in the head. She works in [corporation]⁸ in Bellevue but I don't know where exactly. I don't know if that helps you in someway. She has a 3 years old son that she picks him up at 5 P.M. so she usually gets home around 5ish. Please don't do anything to the boy. That's all. Thanks[.] Send me a proof when the job's done.

24. SOI-1 also provided a picture of VICTIM, which an FBI Special Agent Caryn Highley recognized as VICTIM, having met her in person. Additionally, SOI-1 provided the Bitcoin wallet address used for the transaction, which Agent Highley confirmed on the publicly accessible blockchain received approximately .53 bitcoin on February 4, 2020. Based on the value of Bitcoin on

⁸ This information is redacted to protect VICTIM's privacy and safety. However, I have determined that the corporation listed as VICTIM's employer is, in fact, accurate.

1 that particular date, this amount is roughly equivalent to the amount that SOI-1
2 claimed he/she was paid by the solicitor—\$5,000.

3 **C. Interview of VICTIM**

4 25. On February 13, 2020, Agent Highley, along with others, interviewed
5 VICTIM and advised her of the solicitation of her murder. In order to identify who might
6 have wanted to have VICTIM killed, law enforcement asked VICTIM to identify those
7 who might have wished her harm.

8 26. VICTIM explained that, in 2010, her husband, J.M., was involved in a
9 sexual harassment lawsuit. J.M. alleged that a former employer had harassed him, which
10 led to J.M. leaving his company and suing his former boss. VICTIM felt that it was
11 unlikely that J.M.'s former employer would solicit her murder, but said it was possible
12 due to the "life altering" nature of the situation.

13 27. VICTIM explained that her husband, J.M., was involved in another lawsuit
14 after he left his former employer in October 2019 to form a business. After starting this
15 business, J.M.'s former employer sued J.M. for violation of a non-compete clause. The
16 lawsuit remains ongoing and, in November or December 2019, VICTIM paid their
17 lawyers \$5,000 for legal services from a joint account held by J.M. and VICTIM.
18 Recently, a second payment of \$5,000 had been withdrawn from her husband's business
19 account. VICTIM's husband had informed her that this second payment had been made
20 to their lawyers, since she did not have access to her husband's business account.

21 28. VICTIM also stated that, on December 23, 2019, an unknown female rang
22 VICTIM's front doorbell and asked for J.M. by name. VICTIM's Ring camera captured
23 the interaction. When VICTIM told the female that J.M. was not home, the female said
24 she was there to see VICTIM and asked to come into the house. VICTIM became
25 concerned because the female kept reaching into her pockets. The female's behavior and
26 her desire to enter the residence prompted VICTIM to lock the deadbolt while talking to
27 the unknown female through the door. J.M. was not home, but utilizing the Ring camera,
28 he joined the conversation. Shortly afterward, the female walked away. VICTIM called

1 911 and reported the incident to Bellevue Police Department. She also provided a copy
2 of the video to Bellevue Police Department. VICTIM still had the video footage
3 available. Agent Highley reviewed that video and, due to the image quality, cannot
4 conclusively say the female is FIGUEROA, however, based on the complexion, stature,
5 and voice, the woman in the image appears to resemble FIGUEROA.⁹ At the time,
6 VICTIM did not believe the female knew them. The female asked for J.M. by name, but
7 there was a package outside the residence, next to the front door that was from a family
8 member. The package had J.M.'s full name visible on it, printed in large letters. When
9 the female claimed to be there to see VICTIM, she referred to VICTIM as "you" and
10 never referred to her by name.

11 29. VICTIM also explained that, at the end of January 2020, her employer
12 prematurely ended a contract with a Phoenix-based company. The contract concluded
13 due to work performance issues with this company. VICTIM communicated with an
14 employee of this company, B.O., regularly. According to VICTIM, B.O. is familiar with
15 VICTIM's daily routine, including the time she leaves work to pick up her son. On one
16 occasion, B.O. traveled to Bellevue, Washington, for two weeks to work at VICTIM's
17 employer's office. B.O. and VICTIM had several arguments due to criticism of B.O.'s
18 work performance by VICTIM and her supervisor. B.O. has never threatened VICTIM
19 or any other employees. Despite their turbulent relationship, VICTIM stated she would
20 be surprised if B.O. had tried to harm her. VICTIM last spoke to B.O. on February 12,
21 2020. She said it was difficult to get a hold of B.O., and when she was finally able to
22 contact B.O. on the 12th, B.O. was evasive and quickly ended the phone call.

23 30. When asked about her relationship with her husband, J.M., VICTIM said it
24 had been strained for the last few years. She described it as a "loss of passion" and in
25 2018, VICTIM said her husband asked her for a divorce. She described their relationship
26

27
28 ⁹ As explained below, J.M. later explained that he recognized this person to be FIGUEROA and
FIGUEROA admitted, during a proffer interview, that she was the person on camera.

1 as growing distant, turning into more of a friendship than a marriage. She said this began
2 after her husband went to a Landmark conference. She described the conference as a
3 self-help group designed to help people reassess their lives and make drastic changes.
4 When her husband brought up divorce, VICTIM told her husband that she didn't want to
5 get a divorce. She wanted to remain a family for the sake of their son. She convinced
6 her husband to participate in counseling. However, due to J.M.'s work schedule, he was
7 unable to attend in-person counseling but agreed to an online counseling program.
8 VICTIM stated she had not had an extramarital affair and did not believe her husband
9 had either.

10 31. VICTIM described her and J.M.'s financial situation as strained, due to the
11 new business and the current lawsuit. She described their financial situation as month-to-
12 month. VICTIM stated that she and J.M. each have a \$1.5 million life insurance policy.
13 In December 2019, J.M. began asking her to increase their life insurance policies by five
14 hundred thousand dollars each. VICTIM did not want to meet with an insurance
15 salesman but J.M. continued to bring it up.

16 **D. Interview with J.M.**

17 32. On February 13, 2020, Agent Highley, along with others, interviewed J.M.
18 When informed about the threat, he discussed the current lawsuit involving the non-
19 compete clause. However, he stated it was unlikely that his prior employer would make
20 threats against him or his wife. When discussing the details contained in the threat,
21 provided by SOI-1, he said the timeframe listed for VICTIM coming home was incorrect,
22 as VICTIM usually comes home at a later time of night.

23 33. J.M. asked about VICTIM's work with the Phoenix-based company, noting
24 that "they would be closing that team." He explained that VICTIM had issues with the
25 manager of the Phoenix team (believed to be B.O.) and described the Phoenix manager as
26 "snippy" and "aggressive."

27 34. When describing his job, J.M. stated that he has "great relationships with
28 people at work," his clients "love" him, he "just had a big win" earlier in the day, and

1 does not believe he makes enemies. He stated the “only major points of serious
2 contention are that lawsuit against me and that thing out in Phoenix.”

3 35. When asked if anything unusual had occurred recently, J.M. described the
4 incident from December 23, 2019. VICTIM notified him that someone was at the door
5 asking for him and said that an unknown female asked to enter the residence. He
6 confronted the female through the Ring camera, and was able to pull up video to see what
7 she looked like. J.M. said the female appeared to be older and seemed to be hiding her
8 face. He was unsure of the date but he believed it was after Christmas. The unknown
9 female named him, but not his wife. There was a package outside of the residence that he
10 described as having his name on it, written in large font. The unknown female reminded
11 him of an employee at his former job—the employer involved in the non-compete
12 lawsuit—but said that this employee had been living in Pennsylvania for the last two
13 years. He did not recognize her voice, he described it as having an accent, was unsure of
14 the region, and only described it as an “American” accent.¹⁰ The only other unusual
15 event he could recall was an attempted “break-in” at their residence approximately two
16 years ago.

17 36. When asked about the possibility of the suspect being someone he had a
18 relationship with, J.M. discussed the Landmark personal development course. J.M.
19 explained that he first took a course in 2018, attended a second course in 2019, and began
20 attending the third course near the end of 2019. Due to the length of the third course, he
21 dropped out at the request of his wife because there was too much going on at home.
22 J.M. stated that he provided personal information in group discussions, but never
23 discussed information regarding his or his wife’s schedule. He said he discussed issues
24 about his marriage with people in the group, but also indicated he wanted to repair the
25 marriage. J.M. said he shared the information regarding his wife with a woman, but he
26

27
28 ¹⁰ As described below, J.M. later recanted this explanation and told the FBI that he knew this woman was
FIGUEROA.

1 | could not remember who she was. J.M. said he couldn't imagine that she would
2 | "instigate" the current situation. He stated that he didn't have any "follows" or anyone he
3 | described as a "secret valentines in there or anything. You know what I mean? That I
4 | knew."

5 | 37. During the interview, J.M. initially denied having an extramarital affair. As
6 | the conversation continued, J.M. said there was "someone" at the Landmark program that
7 | "really liked" him. He stated her name was LLUVIA. When asked for her last name,
8 | J.M. accessed his cell phone, and he stated he last had contact with her on January 25,
9 | 2020, when she sent him a paper for him "to correct for school." J.M. explained that
10 | LLUVIA is a student somewhere in South Bend, studying immigration law. Later during
11 | the interview, J.M. accessed LLUVIA FIGUEROA's Facebook account and mentioned
12 | that she was attending school at Grays Harbor College. He claimed the last time
13 | FIGUEROA had been in his house was June 2019.

14 | 38. As the conversation continued, J.M. admitted to having a sexual
15 | relationship with FIGUEROA that lasted approximately "six months or so, a couple
16 | times, here and there." According to J.M., the relationship started as a friendship in 2018
17 | when they met at the Landmark course and later became romantic. He claimed the
18 | romantic relationship ended in August 2019. J.M. said he last saw FIGUEROA in
19 | January of 2020, when she told him she still loved him.

20 | 39. J.M. explained that, while he knew FIGUEROA, he provided her with
21 | money on multiple occasions to "help her out." Most recently, on January 3, 2020,
22 | FIGUEROA asked J.M. for \$5,000. J.M. said that he didn't have that amount of money
23 | and instead gave her \$2,000. FIGUEROA said that the money was to help her parents
24 | because they were victims of a break-in and lost their life savings. While all of the
25 | previous payments were sent through Facebook, the \$2,000 payment was made through
26 | J.M.'s PayPal account.

27 | 40. When the situation in Phoenix was brought up again, J.M. stated, "No, I
28 | don't think that, I mean, if anything it's this [his relationship with FIGUEROA], this is

1 much more probabl[e] than that.” When asked why he felt that way, J.M. stated it was
2 because, “[FIGUEROA] likes me and I said, I’m not gonna do that anymore...”
3 However, J.M. clarified that FIGUEROA gave him no indication of being a threat.

4 **E. Interview of FIGUEROA**

5 41. On February 14, 2020, FBI Special Agent Schroff interviewed LLUVIA
6 FIGUEROA¹¹ at her place of employment in Aberdeen, Washington. Prior to the
7 interview, Agent Schroff identified himself with his FBI credentials and asked
8 FIGUEROA if she would be willing to speak with him in a private place. Agent Schroff
9 informed FIGUEROA that she wasn’t in trouble but may be a witness. FIGUEROA
10 agreed and suggested the two meet outside as there were no quiet semi-private areas
11 inside the business. Due to the temperature outside, Agent Schroff suggested the two
12 speak in his vehicle and asked FIGUEROA if she would be comfortable with that.
13 FIGUEROA agreed and the two spoke in the vehicle, with FIGUEROA sitting in the
14 passenger seat of the unlocked car. Towards the end of the interview, Agent Schroff
15 explicitly told FIGUEROA that she was not under arrest and would be going back to
16 work that night.

17 42. FIGUEROA told Agent Schroff that she participated in the Landmark
18 program, along with her brother, and met J.M. there. They became friends, and their
19 friendship evolved into a sexual relationship that has continued. FIGUEROA said that
20 she had been in J.M.’s house five to seven times, including once with her brother.
21 FIGUEROA explained that she last saw J.M. approximately three weeks ago when they
22 went to Portland, Oregon, where they spent the night.

23 43. FIGUEROA claimed that, at first, she was unaware that J.M. was married.
24 When she found out, J.M. told FIGUEROA that his wife had cancer and that he talked to
25 his wife about divorce but decided to stay with her due to her illness. FIGUEROA stated
26
27

28 ¹¹ This interview was recorded surreptitiously.
AFFIDAVIT OF SPECIAL AGENT KLEINOSKY- 15
USAO# 2020R00187

1 the situation made her angry. FIGUEROA initially denied hiring someone to hurt J.M.'s
2 wife.

3 44. Agent Schroff asked FIGUEROA for further details about J.M.
4 FIGUEROA explained that, even though she knew J.M. for approximately two years, she
5 did not believe she knew him completely. When asked why she felt that way,
6 FIGUEROA stated that J.M. would say things that were not accurate. For example,
7 FIGUEROA said that J.M. told her that his wife was sick, and that he could not stand his
8 wife. However, FIGUEROA observed photos online of J.M. and his wife that appeared
9 to contradict those statements. Additionally, when J.M. and FIGUEROA went to Oregon
10 together, J.M. told FIGUEROA that his wife went to Malaysia to get surgery.
11 FIGUEROA learned that VICTIM took her son with her to Malaysia, and FIGUEROA
12 thought that a sick woman would likely not travel internationally with a child.
13 FIGUEROA believed that J.M.'s son was approximately two or three years old.
14 FIGUEROA knew the three-year-old went to school in Bellevue, Washington, but she did
15 not know where.

16 45. FIGUEROA said that in November or December 2019, she "tried to send
17 [VICTIM] some images" on Facebook "about [the relationship between J.M.] and I."
18 FIGUEROA also said that, several years ago, she and her friend created a fake Facebook
19 account but claimed that she hadn't done so recently.

20 46. Although earlier in the interview FIGUEROA repeatedly denied trying to
21 murder VICTIM, as the conversation continued, FIGUEROA admitted that she solicited
22 the murder. FIGUEROA explained that "[t]he person that did that, it was me, I don't
23 know this would help right now or not, but I tried to delete it, but I couldn't do it..."
24 FIGUEROA said that she had used an "old phone" to solicit the hit, downloading an
25 application on her phone to hide her identity. Based on my training and experience, and
26 information conveyed by FIGUEROA, I believe this application is a Tor browser, used to
27 access the dark web. FIGUEROA explained that she purchased the services of an
28 unknown individual to kill VICTIM, and paid for those services with \$5,000 in bitcoin.

1 FIGUEROA had previously explained that she was familiar with Bitcoin because she
2 used it to purchase clothes from another country. FIGUEROA explained that there was
3 an option on the website, where she had solicited the hit, to “delete” the transaction, but
4 she was unable to do so because she could no longer access the website on her phone.

5 47. FIGUEROA believed there was a “fifteen-fifty” chance that the website
6 offering hitman services was a scam. When asked how FIGUEROA felt about VICTIM
7 being killed, she stated she was nervous. When asked if she hoping J.M. would come
8 live with her once his wife was killed, FIGUEROA said “...yeah.” FIGUEROA denied
9 that J.M. was involved in the plan to murder his wife. FIGUEROA said the phone she
10 used to solicit the murder was currently at her home, in her bedroom in South Bend,
11 Washington. She stated that she deleted her browser history on the phone and had not
12 discussed the incident with anyone else.

13 48. On February 21, 2020, Agent Schroff and I tried to interview FIGUEROA
14 again but she invoked her right to counsel and declined to be interviewed. As described
15 herein, FIGUEROA later participated in a proffer interview on March 17, 2020.

16 **F. VICTIM’s Facebook Account**

17 49. I have reviewed VICTIM’s Facebook account, with her consent, and
18 located messages sent from an account held in the name of Katlyn Everson. When
19 viewing this account publicly, neither a profile picture nor a cover photo are shown for
20 Katlyn Everson. It appeared that VICTIM had not yet accessed or opened these
21 messages at the time that I viewed them.

22 50. On December 17, 2019, the Everson account sent VICTIM a series of
23 messages. First, the Everson account sent VICTIM a photograph of J.M., followed by a
24 message that stated “I know it’s none of my business but [J.M] Im guessing your husband
25 is cheating on u. I know it because I know the person he’s cheating on u with. If u dont
26 believe me, they’re gonna meet up today at the Kizuki Ramen restaurant in Olympia at
27 4:30 PM. You can prove it by yourself.”
28

1 51. On January 2, 2020, the Everson account sent VICTIM a series of pictures,
2 which appear to show J.M. kissing and sitting next to FIGUEROA, taken by what
3 appears to be a third party at a neighboring table in the restaurant.

4 52. I showed VICTIM a copy of the photograph provided to SOI-1, when the
5 individual solicited VICTIM's murder. VICTIM confirmed that this photograph is
6 publicly accessible on VICTIM's Facebook page.

7 **G. Follow-Up Interview of J.M.**

8 53. March 3, 2020, I interviewed J.M. During this interview, I again asked him
9 about the Ring camera video, taken on December 23, 2019, when an unknown female
10 rang VICTIM's front doorbell and asked for J.M. by name. J.M. admitted that he knew
11 the woman in the video was FIGUEROA and that he had previously lied to investigators
12 when he denied recognizing the individual in the video. J.M. stated that, after this video
13 was taken, he talked to FIGUEROA and asked her why she had gone to his home.
14 FIGUEROA told J.M. that she was there to kill VICTIM and that she brought a knife
15 with her in order to accomplish the murder.

16 54. J.M. said that he had omitted this information from his prior interview
17 because he was concerned his wife would find out about the affair. J.M. made the
18 following statement regarding the time frame of his relationship with FIGUEROA, which
19 he did not disclose to law enforcement during his first interview. J.M. started a friendship
20 with FIGUEROA and her brother in August of 2018. J.M. stated that the relationship
21 evolved into a sexual relationship in the beginning of 2019. J.M. said he ended the
22 romantic relationship with FIGUEROA in the summer of 2019 but maintained a
23 friendship with her. J.M. stated that the relationship became romantic again in December
24 of 2019. J.M. stated that, the last time he saw FIGUEROA was on January 28, 2020,
25 when they met for dinner.

26 **H. FIGUEROA Proffer Interview**

27 55. On March 17, 2020, I, along with others, interviewed FIGUEROA pursuant
28 to a proffer agreement, in the presence of her counsel.

1 56. During this proffer interview FIGUEROA confirmed that she had solicited
2 VICTIM's murder. FIGUEROA explained that she had been having an affair with
3 VICTIM's husband, J.M., since approximately the summer of 2018. FIGUEROA
4 explained that their relationship ebbed and flowed, with FIGUEROA ending the
5 relationship at multiple points after FIGUEROA became frustrated that J.M. would not
6 leave his wife.

7 57. FIGUEROA explained that J.M. offered several excuses for why he would
8 not leave his wife, including that his wife had cancer, he was afraid that he would lose
9 custody of his child in a divorce, and that his wife had tried to take her life when he
10 previously threatened her with divorce. FIGUEROA claimed that J.M. told her that they
11 could not be together until his wife died or something happened.

12 58. FIGUEROA stated that she and J.M. rekindled their romance for the final
13 time in the fall of 2019. After returning to her relationship with J.M., FIGUEROA took
14 several steps to try to end J.M. and VICTIM's marriage.

15 59. First, FIGUEROA tried to send VICTIM pictures of herself and J.M. being
16 intimate at a restaurant. To do this, FIGUEROA set up a fake Facebook account and sent
17 pictures to VICTIM. These pictures were taken by FIGUEROA's cousin, who was
18 seated at a nearby table when J.M. and FIGUEROA were having dinner. FIGUEROA
19 asked her cousin to take these photographs so she could send them to VICTIM. After
20 sending these photographs, FIGUEROA received no response from VICTIM.

21 60. FIGUEROA then escalated her behavior, deciding to go to VICTIM's
22 home to tell her in person about the affair. FIGUEROA and J.M. made plans to meet for
23 dinner at a restaurant in Olympia. Knowing that J.M. would be on his way to the
24 restaurant, FIGUEROA went to VICTIM's house and told VICTIM that she was looking
25 for J.M. When VICTIM said that J.M. was not home, FIGUEROA explained that she
26 had something to tell VICTIM. At that point, J.M. started speaking to FIGUEROA using
27 the Ring camera connected to VICTIM's home and FIGUEROA decided to leave.
28

61. FIGUEROA explained that, after leaving the house, FIGUEROA met J.M. for dinner. J.M. asked why FIGUEROA went to his home, and FIGUEROA told him that she went there to kill VICTIM. FIGUEROA stated that she did not really intend to kill VICTIM, and was not armed when she went to the home, but told J.M. this because she was upset. FIGUEROA claimed that J.M. wasn't angry but instead saw the behavior as a sign of her dedication and affection for him.

62. FIGUEROA claimed that, in the past, J.M. had made comments about wanting to kill his wife and once asked FIGUEROA if she knew anyone who would kill his wife.

63. FIGUEROA confirmed that J.M. had previously sent her money using Facebook messenger and recently sent her \$2,000 using PayPal. FIGUEROA explained that she used this \$2,000, along with money she had saved from her college scholarship, to solicit VICTIM's murder. FIGUEROA said that J.M. did not know that she planned on hiring a hitman on the dark web, but believed that J.M. would be pleased if he found out that she had.

64. FIGUEROA stated that, to solicit the murder, she used her old phone, a phone that she had obtained from her pastor that was not linked to her. She then googled the dark web, downloaded an application to access the dark web, and located several sites offering hitmen services. FIGUEROA studied those sites, reviewing comments and requesting information on pricing, before selecting her hitman. FIGUEROA explained that these sites offered a multitude of services, offering to beat, maim, or kill victims, to be carried out by hitmen with a range of experience levels. She selected SOI-1's site because it had an escrow system, giving her a sense of security that her funds would not be stolen. FIGUEROA explained that, to solicit the hit, she sent a message to SOI-1 on this website, sending SOI-1 VICTIM's Facebook profile picture, VICTIM's name and address, requesting that SOI-1 shoot VICTIM in the head, telling SOI-1 that she would release the funds from escrow once she had a picture of the VICTIM murdered, and asking SOI-1 not to harm VICTIM's child.

1 65. To obtain the \$5,000 in bitcoin necessary to pay for the hit, FIGUEROA
2 explained that she went to a number of websites that offered bitcoin wallet services.
3 FIGUEROA used fake names and email addresses on these websites. FIGUEROA said
4 that she went to multiple websites, stopping after each site asked her for identifying
5 information or a copy of her driver's license. Finally, she found a website that didn't ask
6 her for any identifying information, and FIGUEROA opened a wallet on that site using a
7 fake email address that began with the name Nicole, believed by law enforcement to be
8 nicolestigall22@outlook.com.

9 66. To purchase the bitcoin, FIGUEROA went to a bitcoin ATM, located
10 outside a gas station in Olympia, Washington. After FIGUEROA put cash into this ATM
11 and scanned her wallet address, bitcoin was transferred to her wallet. FIGUEROA went
12 to this ATM twice in order to obtain enough bitcoin to pay for the hit. FIGUEROA then
13 transferred this bitcoin to a wallet address provided by SOI-1.

14 67. After paying these funds, FIGUEROA claimed that weeks went by and
15 SOI-1 had still not murdered VICTIM. FIGUEROA went back to SOI-1's website and
16 asked him/her about the delay. SOI-1 told FIGUEROA that the hitman who had been
17 hired was arrested and they were going to staff another hitman to complete the hit.

18 68. In addition to contacting SOI-1, FIGUEROA explained that she also
19 contacted a second hitman, communicating with this hitman via email. FIGUEROA sent
20 that hitman VICTIM's photograph and address but declined to use that hitman's services
21 because he/she was more expensive and less reliable than SOI-1.

22 **I. THE SUBJECT ACCOUNTS**

23 69. While they were having an affair, FIGUEROA and J.M. communicated
24 using **SUBJECT ACCOUNT 1**.

1 a. For example, on October 9, 2018, J.M. emailed FIGUEROA, using
2 the email address lfigueroa@my.ghc.edu (**SUBJECT ACCOUNT 1**).¹²

3 b. Additionally, on November 23, 2019, lfigueroa@my.ghc.edu
4 (**SUBJECT ACCOUNT 1**) sent an email to J.M.

5 70. During the time period of the affair, J.M. and FIGUEROA also used
6 Facebook to communicate and so that J.M. could send money to FIGUEROA.

7 a. FIGUEROA used the account lluviaselene.sierrafigueroa.
8 According to Facebook, this account was registered in the name of LLUVIA
9 FIGUEROA on May 23, 2011.

10 b. From September 2018 through August 2019, FIGUEROA,
11 used this Facebook account to exchange messages with J.M. FIGUEROA also
12 had payment information registered to their accounts.

13 c. **SUBJECT ACCOUNTS 2 and 3** are listed as two of three
14 registered email addresses associated with FIGUEROA's Facebook account.

15 d. Based on my training and experience, I know that if an
16 individual sends a Facebook message—a private direct message only visible to the
17 Facebook sender and recipient—Facebook will often email the recipient
18 notifications when the user has received a message. This includes notifications
19 that a Facebook user has received a payment using Facebook Messenger
20 payments. Additionally, Facebook will notify user if they have been tagged on
21 another's page or mentioned in another's post. These notifications can include the
22 substance of another's tag or Facebook post. **SUBJECT ACCOUNTS 2 and 3**
23 would have received these kinds of communications from Facebook.

24
25
26
27 ¹² FIGUEROA is a student at Grays Harbor College. As described herein, this account is serviced by Microsoft.
28 Law enforcement previously obtained a warrant to obtain this information from Microsoft but Microsoft requested
that we gather the emails directly from Grays Harbor College. Accordingly, I seek this additional warrant to obtain
information related to this account from Grays Harbor College.

1 e. For example, on April 3, 2020, **SUBJECT ACCOUNT 2**
2 received a message from “The Messenger Team” at
3 notification@facebookmail.com. Additionally, on October 11, 2019, **SUBJECT**
4 **ACCOUNT 2** received a message from “Facebook” at
5 notification@facebookmail.com.

6 71. FIGUEROA also obtained emails from financial institutions at
7 **SUBJECT ACCOUNT 2**. These emails may help identify FIGUEROA’s assets,
8 the location of her accounts, and receipt of funds from J.M. or other sources, used
9 to pay SOI-1.

10 a. For example, on December 28, 2019 and January 21, 2020,
11 **SUBJECT ACCOUNT 2** received emails from operations@ssbwa.com, affiliated
12 with Security State Bank.

13 b. Additionally, during her proffer, FIGUEROA stated that she
14 used a portion of her academic scholarship to pay the remaining \$5,000 to SOI-1.
15 **SUBJECT ACCOUNT 2** also contains emails from Grays Harbor College,
16 including an email on November 22, 2019 from cashier@ghc.edu.

17 72. In order to gather information related to FIGUEROA’s efforts to
18 solicit VICTIM’s murder, including evidence that FIGUEROA was having an
19 affair with J.M., FIGUEROA accepted money from J.M., and FIGUEROA used
20 this money along with her scholarship funds to solicit VICTIM’s murder, I request
21 authorization to search the **SUBJECT ACCOUNTS**.

22 **BACKGROUND CONCERNING ONLINE ACCOUNTS**

23 73. As explained herein, information stored in connection with an online
24 account may provide crucial evidence of the “who, what, why, when, where, and how” of
25 the criminal conduct under investigation, thus enabling the United States to establish and
26 prove each element or alternatively, to exclude the innocent from further suspicion.

27 74. In my training and experience, the information stored in connection with an
28 online account can indicate who has used or controlled the account. This “user

1 attribution” evidence is analogous to the search for “indicia of occupancy” while
2 executing a search warrant at a residence. For example, email communications, contacts
3 lists, and images sent (and the data associated with the foregoing, such as date and time)
4 may indicate who used or controlled the account at a relevant time.

5 75. Further, information maintained by the email provider can show how and
6 when the account was accessed or used. For example, as described below, email
7 providers typically log the Internet Protocol (IP) addresses from which users access the
8 email account, along with the time and date of that access. By determining the physical
9 location associated with the logged IP addresses, investigators can understand the
10 chronological and geographic context of the email account access and use relating to the
11 crime under investigation. This geographic and timeline information may tend to either
12 inculcate or exculpate the account owner. Additionally, information stored at the user’s
13 account may further indicate the geographic location of the account user at a particular
14 time (e.g., location information integrated into an image or video sent via email).

15 76. Stored electronic data may provide relevant insight into the email account
16 owner’s state of mind as it relates to the offense under investigation. For example,
17 information in the email account may indicate the owner’s motive and intent to commit a
18 crime (e.g., communications relating to the crime), or consciousness of guilt (e.g.,
19 deleting communications in an effort to conceal them from law enforcement).

20 1. Microsoft’s and Grays Harbor College’s Services

21 77. In my training and experience, I have learned that Microsoft provides a
22 variety of online services, including electronic mail (“email”) access and instant
23 messaging (otherwise known as “chat” messaging), to the general public. Microsoft
24 provides subscribers email and chat accounts at the domain name “@hotmail.com.”

25 78. According to online databases, Microsoft services the domain @
26 my.ghc.edu, on behalf of Grays Harbor College. Grays Harbor College also keeps
27 copies of these records.
28

A. Subscriber Records and Account Content

79. Subscribers obtain an account by registering with Microsoft. When doing so, email providers like Microsoft ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

80. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Microsoft's websites), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

81. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

1 evidence of the crimes under investigation because the information can be used to
2 identify the account's user or users.

3 82. In general, an email that is sent to a Microsoft subscriber is stored in the
4 subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email.
5 When the subscriber sends an email, it is initiated at the user's computer, transferred via
6 the Internet to Microsoft servers, and then transmitted to its end destination. Microsoft
7 often maintains a copy of received and sent emails. Unless the sender specifically deletes
8 an email from the Microsoft server, the email can remain on the system indefinitely.
9 Even if the subscriber deletes the email, it may continue to be available on Microsoft's
10 servers for some period of time.

11 83. A sent or received email typically includes the content of the message,
12 source and destination addresses, the date and time at which the email was sent, and the
13 size and length of the email. If an email user writes a draft message but does not send it,
14 that message may also be saved by Microsoft but may not include all of these categories
15 of data.

16 84. In my training and experience email providers like Microsoft typically
17 retain certain transactional information about the creation and use of each account on
18 their systems. This information can include the date on which the account was created,
19 the length of service, records of log-in (*i.e.*, session) times and durations, the types of
20 service utilized, the status of the account (including whether the account is inactive or
21 closed), the methods used to connect to the account (such as logging into the account via
22 a website), and other log files that reflect usage of the account. In addition, email
23 providers often have records of the IP address used to register the account and the IP
24 addresses associated with particular logins to the account. Because every device that
25 connects to the Internet must use an IP address, IP address information can help to
26 identify which computers or other devices were used to access the email account, which
27 can help establish the individual or individuals who had dominion and control over the
28 account

1 85. In general, an email that is sent to a Microsoft subscriber is stored in the
2 subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If
3 the subscriber does not delete the message, the message can remain on Microsoft's
4 servers indefinitely. Even if the subscriber deletes the email, it may continue to be
5 available on Microsoft's servers for a certain period of time.

6 86. When the subscriber sends an email, it is initiated at the user's computer,
7 transferred via the Internet to Microsoft's servers, and then transmitted to its end
8 destination. Microsoft often maintains a copy of the email sent. Unless the sender of the
9 email specifically deletes the email from Microsoft's server, the email can remain on the
10 system indefinitely. Even if the sender deletes the email, it may continue to be available
11 on Microsoft's servers for a certain period of time.

12 87. A sent or received email typically includes the content of the message,
13 source and destination addresses, the date and time at which the email was sent, and the
14 size and length of the email. If an email user writes a draft message but does not send it,
15 that message may also be saved by Microsoft but may not include all of these categories
16 of data.

17 88. Microsoft provides a variety of online, or "cloud," services in addition to
18 email access, to the public and to customers who utilize Hotmail accounts that are served
19 by Microsoft. Microsoft's various cloud services are associated with a single Microsoft
20 account, which is typically associated with a Microsoft email address, but can be
21 associated with any email address. The various cloud services provided by Microsoft are
22 optional and can be turned "on" or "off" by the user.

23 89. In providing services such as Outlook, OneDrive, Xbox, calendar services,
24 online file storage, storage of browsing history, storage of search history, and locations
25 history, Microsoft collects information that constitute evidence of the crimes under
26 investigation. For example, such evidence can be used to discover or confirm the identity
27 and location users of the service at a particular time.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

90. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to require **THE PROVIDERS**, and their agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to **THE PROVIDERS** with direction that they identify the accounts described in Attachments A-1 and A-2 to this affidavit, as well as other subscriber and log records associated with the accounts, as set forth in Section I of Attachments B-1 and B-2 to this affidavit.

91. The search warrant will direct **THE PROVIDERS** to create an exact copy of the specified account and records.

92. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachments B-1 and B-2 for seizure.

93. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of “hits,” each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant “hit” does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and

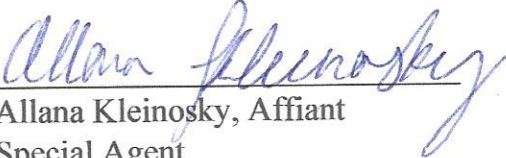
1 methodologies reasonably designed to identify and seize the items identified in Section II
2 of Attachments B-1 and B-2 to the warrant.

3 94. Based on my experience and training, and the experience and training of
4 other agents with whom I have communicated, it is necessary to review and seize a
5 variety of e-mail communications, chat logs and documents, that identify any users of the
6 subject account and e-mails sent or received in temporal proximity to incriminating e-
7 mails that provide context to the incriminating communications.


8 CONCLUSION

9 95. Based on the forgoing, I respectfully request that the Court issue the
10 proposed search warrant. This Court has jurisdiction to issue the requested warrant
11 because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18
12 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of
13 the United States . . . that - has jurisdiction over the offense being investigated.” 18
14 U.S.C. § 2711(3)(A)(i). Additionally, the Court “is in . . . a district in which the provider
15 . . . is located or in which the wire or electronic communications, records, or other
16 information are stored.” 18 U.S.C. § 2711(3)(A)(ii). Pursuant to 18 U.S.C. § 2703(g), the
17 presence of a law enforcement officer is not required for the service or execution of this
18 warrant.

1 96. Accordingly, by this Affidavit and Warrant I seek authority for the
2 government to search all of the items specified in Section I, Attachments B-1 and B-2
3 (attached hereto and incorporated by reference herein) to the Warrant, and specifically to
4 seize all of the data, documents and records that are identified in Section II to that same
5 Attachment.

6
7 
8 Allana Kleinosky, Affiant
9 Special Agent

10 The above-named agent provided a sworn statement attesting to the truth of the
11 foregoing affidavit on the 23 day of April, 2020.

12
13 
14 HONORABLE BRIAN A. TSUCHIDA
15 United States Magistrate Judge
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A-1

Grays Harbor College Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Grays Harbor College account:

lfigueroa@my.ghc.edu

(the "Account") that are stored at a premises controlled by Grays Harbor College, a school that accepts service of legal process at 1620 Edward P. Smith Drive in Aberdeen, Washington.

ATTACHMENT B-1**Particular Things to be Seized****I. Information to be disclosed by Grays Harbor College:**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Grays Harbor College, including any data, messages, records, files, logs, or information that has been deleted but is still available to Grays Harbor College, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Grays Harbor College is required to disclose the following information to the government for each Account or identifier listed in Attachment A-1, from June 1, 2018 to the present:

a. All electronic mail content and/or preserved data (including email, attachments, and embedded files);

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as IP address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. all contact lists;

d. all account history, including any records of communications between Grays Harbor College and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

Grays Harbor College is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Section 1958 (Murder for Hire), those violations occurring between June 2018 and the present, for each of the Accounts listed on Attachment A-1, including the following:

a. any information related to J.M.'s relationship with FIGUEROA, including communications between the two, plans to meet, and photographs of FIGUEROA and J.M.;

b. any information related to romantic feelings between J.M. and FIGUEROA, desire to remain a couple, or desire to break up or end their affair;

c. any information related to FIGUEROA's desire to have J.M. end his marriage or to marry or solely be romantically involved with FIGUEROA.

d. any information related to J.M.'s relationship with VICTIM, including communications regarding divorce, separation, or illness, or evidence that J.M. was unhappy in his marriage or sought to murder VICTIM;

e. any information related to a plan to solicit murder, including by accessing websites or contacting individuals to solicit murder;

f. any information related to J.M.'s or FIGUEROA's attendance at a Landmark course or FIGUEROA's attempts to visit or actual visits to VICTIM's house;

g. any information related to payments made by J.M. to FIGUEROA;

h. any information related to FIGUEROA's transfer, purchase, sale, or disposition of Bitcoin or other cryptocurrency;

i. any information related to J.M.'s or FIGUEROA's assets, including their bank records, checks, credit card bills, account information, scholarship funds, and other financial records, to include life insurance policies.

1 j. any information related to use of the dark web, including use or
2 downloading of a Tor browser;

3 k. any information related to J.M.'s statements to FIGUEROA
4 regarding VICTIM;

5 l. any information related to efforts to delete browsing history or
6 undertake other acts to remain anonymous online, including by accessing VPNs or
7 creating multiple email accounts in a short time frame;

8 m. any information related to the creation of a fake Facebook account to
9 contact VICTIM or fake email accounts to use in furtherance of the solicitation for
10 murder;

11 n. any information related to prior attempts to harm or threaten
12 VICTIM, or to reveal J.M.'s and FIGUEROA's affair;

13 o. any information consisting of, referring to, or reflecting use of
14 cryptocurrency, including cryptocurrency client software, cryptocurrency wallet files, and
15 related private encryption keys, seed phrases, or other passwords;

16 p. any information consisting of, referring to, or reflecting use of
17 encryption or digital signature software, such as PGP encryption, and related public and
18 private encryption keys;

19 q. any information related to cryptocurrency applications and wallets,
20 to include information regarding current account balance and transaction history, *i.e.*,
21 date, time, amount, an address of the sender/recipient of a cryptocurrency transaction
22 maintained in such wallets;

23 r. any information reflecting cryptocurrencies, including web history,
24 and documents showing the location, source, and timing of acquisition of any
25 cryptocurrencies, to include wallets, wallet addresses, and seed phrases; and

26 s. Evidence that serves to identify any person who uses or accesses the
27 Account or who exercises in any way any dominion or control over the Account;
28

1 t. Evidence that may identify the aliases names, online user names,
2 “handles” and/or “nics” of those who exercise in any way any dominion or control over
3 the specified Account as well as records or information that may reveal the true identities
4 of these individuals;

5 u. Other log records, including IP address captures, associated with the
6 specified Account;

7 v. Subscriber records associated with the specified Account, including
8 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session
9 times and durations; 4) length of service (including start date) and types of services
10 utilized; 5) telephone or instrument number or other subscriber number or identity,
11 Including any temporarily assigned network address such as IP address, media access
12 card addresses, or any other unique device identifiers recorded by internet service
13 provider in relation to the account; 6) account log files (login IP address, account
14 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
15 and source of payment; and 9) lists of all related accounts;

16 w. Records of communications between the internet service provider
17 and any person purporting to be the account holder about issues relating to the Account,
18 such as technical problems, billing inquiries, or complaints from other users about the
19 specified Account. This to include records of contacts between the subscriber and the
20 provider’s support services, as well as records of any actions taken by the provider or
21 subscriber as a result of the communications.

22 x. Information identifying accounts that are linked or associated with
23 the Account.

24
25 This warrant authorizes a review of electronically stored information,
26 communications, other records and information disclosed pursuant to this warrant in
27 order to locate evidence, fruits, and instrumentalities described in this warrant. The
28 review of this electronic data may be conducted by any government personnel assisting in

1 the investigation, who may include, in addition to law enforcement officers and agents,
2 attorneys for the government, attorney support staff, and technical experts. Pursuant to
3 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
4 custody and control of attorneys for the government and their support staff for their
5 independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by
the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the
information contained in this certification is true and correct. I am employed by
_____, and my title is _____. I am
qualified to authenticate the records attached hereto because I am familiar with how the
records were created, managed, stored, and retrieved. I state that the records attached
hereto are true duplicates of the original records in the custody of _____.

The attached records consist of _____ [GENERALLY DESCRIBE
RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time
of the occurrence of the matter set forth by, or from information transmitted by, a person
with knowledge of those matters, they were kept in the ordinary course of the regularly
conducted business activity of _____, and they were made by
_____ as a regular practice; and

b. such records were generated by _____'s electronic
process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or
file(s) in the custody of _____ in a manner to ensure that they are true
duplicates of the original records; and

2. the process or system is regularly verified by _____, and at
all times pertinent to the records certified here the process and system functioned
properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of
the Federal Rules of Evidence.

Date Signature

AFFIDAVIT OF SPECIAL AGENT KLEINOSKY- 37
USAO# 2020R00187

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Microsoft Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Microsoft accounts:

prinhces_latina07@hotmail.com

lluvia_selene07@hotmail.com

(the “Accounts”) that are stored at a premises controlled by Microsoft Corporation, a company that accepts service of legal process at 1 Microsoft Way in Redmond, Washington.

ATTACHMENT B-2**Particular Things to be Seized****I. Information to be disclosed by Microsoft Corporation:**

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Microsoft Corporation ("Microsoft"), including any data, messages, records, files, logs, or information that has been deleted but is still available to Microsoft, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A-2, from June 2018 to the present:

a. All electronic mail content and/or preserved data (including email, attachments, and embedded files);

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as IP address, media access card addresses, or any other unique device identifiers recorded by Microsoft in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. all contact lists;

i. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during

1 registration, methods of connecting, log files, and means and source of payment
 2 (including any credit or bank account number);

3 j. The types of service utilized;

4 k. All records or other information stored at any time by an individual using
 5 the account, including address books, contact and buddy lists, calendar data, pictures, and
 6 files;

7 l. All account history, including any records of communications between
 8 Microsoft and any other person about issues relating to the accounts, such as technical
 9 problems, billing inquiries, or complaints from other users about the specified account.
 10 This to include records of contacts between the subscriber and the provider's support
 11 services, as well as records of any actions taken by the provider or subscriber in
 12 connection with the service.

13 Microsoft is hereby ordered to disclose the above information to the government
 14 within **14 days** of service of this warrant.

16 **II. Information to be seized by the government**

17 All information described above in Section I that constitutes fruits, contraband,
 18 evidence and instrumentalities of violations of Title 18, United States Code, Section 1958
 19 (Murder for Hire), those violations occurring between June 2018 and the present, for each
 20 of the Accounts listed on Attachment A-2, including the following:

21 a. any information related to J.M.'s relationship with FIGUEROA,
 22 including communications between the two, plans to meet, and photographs of
 23 FIGUEROA and J.M. (together or held by or sent to the other);

24 b. any information related to romantic feelings between J.M. and
 25 FIGUEROA, desire to remain a couple, or desire to break up or end their affair;

26 c. any information related to FIGUEROA's desire to have J.M. end his
 27 marriage or to marry or solely be romantically involved with FIGUEROA.

1 d. any information related to J.M.'s relationship with VICTIM,
2 including communications regarding divorce, separation, or illness, or evidence that J.M.
3 was unhappy in his marriage or sought to murder VICTIM;

4 e. any information related to a plan to solicit murder, including by
5 accessing websites or contacting individuals to solicit murder;

6 f. any information related to J.M.'s or FIGUEROA's attendance at a
7 Landmark course or FIGUEROA's attempts to visit or actual visits to VICTIM's house;

8 g. any information related to payments made by J.M. to FIGUEROA;

9 h. any information related to FIGUEROA's transfer, purchase, sale, or
10 disposition of Bitcoin or other cryptocurrency;

11 i. any information related to J.M.'s or FIGUEROA's assets, including
12 their bank records, checks, credit card bills, account information, and other financial
13 records, to include life insurance policies.

14 j. any information related to use of the dark web, including use or
15 downloading of a Tor browser;

16 k. any information related to J.M.'s statements to FIGUEROA
17 regarding VICTIM;

18 l. any information related to efforts to delete browsing history or
19 undertake other acts to remain anonymous online, including by accessing VPNs or
20 creating multiple email accounts in a short time frame;

21 m. any information related to the creation of a fake Facebook account to
22 contact VICTIM or fake email accounts to use in furtherance of the solicitation for
23 murder;

24 n. any information related to prior attempts to harm or threaten
25 VICTIM, or to reveal J.M.'s and FIGUEROA's affair;

26 o. any information consisting of, referring to, or reflecting use of
27 cryptocurrency, including cryptocurrency client software, cryptocurrency wallet files, and
28 related private encryption keys, seed phrases, or other passwords;

1 p. any information consisting of, referring to, or reflecting use of
2 encryption or digital signature software, such as PGP encryption, and related public and
3 private encryption keys;

4 q. any information related to cryptocurrency applications and wallets,
5 to include information regarding current account balance and transaction history, *i.e.*,
6 date, time, amount, an address of the sender/recipient of a cryptocurrency transaction
7 maintained in such wallets;

8 r. any information reflecting cryptocurrencies, including web history,
9 and documents showing the location, source, and timing of acquisition of any
10 cryptocurrencies, to include wallets, wallet addresses, and seed phrases; and

11 s. Evidence that serves to identify any person who uses or accesses the
12 Accounts or who exercises in any way any dominion or control over the Accounts;

13 t. Evidence that may identify the aliases names, online user names,
14 “handles” and/or “nics” of those who exercise in any way any dominion or control over
15 the specified Accounts as well as records or information that may reveal the true
16 identities of these individuals;

17 u. Other log records, including IP address captures, associated with the
18 specified Accounts;

19 v. Subscriber records associated with the specified Accounts, including
20 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session
21 times and durations; 4) length of service (including start date) and types of services
22 utilized; 5) telephone or instrument number or other subscriber number or identity,
23 Including any temporarily assigned network address such as IP address, media access
24 card addresses, or any other unique device identifiers recorded by internet service
25 provider in relation to the account; 6) account log files (login IP address, account
26 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
27 and source of payment; and 9) lists of all related accounts;

1 w. Records of communications between the internet service provider
2 and any person purporting to be the account holder about issues relating to the Accounts,
3 such as technical problems, billing inquiries, or complaints from other users about the
4 specified Accounts. This to include records of contacts between the subscriber and the
5 provider's support services, as well as records of any actions taken by the provider or
6 subscriber as a result of the communications.

7 x. Information identifying accounts that are linked or associated with
8 the Accounts.

9
10 This warrant authorizes a review of electronically stored information,
11 communications, other records and information disclosed pursuant to this warrant in
12 order to locate evidence, fruits, and instrumentalities described in this warrant. The
13 review of this electronic data may be conducted by any government personnel assisting in
14 the investigation, who may include, in addition to law enforcement officers and agents,
15 attorneys for the government, attorney support staff, and technical experts. Pursuant to
16 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
17 custody and control of attorneys for the government and their support staff for their
18 independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by _____, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of _____.

The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of _____, and they were made by _____ as a regular practice; and

b. such records were generated by _____'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of _____ in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by _____, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date _____ Signature _____

AFFIDAVIT OF SPECIAL AGENT KLEINOSKY- 44
USAO# 2020R00187

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970